WHAT IS CLAIMED IS:

1. A method for protecting a specific one of a program area and a dada area having specific usage standards to be applied to a basic input/output system (BIOS), wherein said basic input/output system defines a mapping table therein, said method comprising steps of:

providing at least one product and reading a product characteristic value of said at least one product;

operating said product characteristic value through an algorithm to obtain an operation value;

comparing said operation value with said mapping table to decide whether said at least one product has said characteristic value conforming to said usage standards of said specific one of said program area and said data area; and

executing a protection action for said specific one of said program area and said data area when said at least one product does not have said characteristic value conforming to said usage standards of said specific one of said program area and said data area, thereby preventing said specific one of said program area and said data area from being misappropriated illegally.

2. A method according to claim 1 wherein said product characteristic value is obtained via reading contents of said at least one product.

3. A method according to claim 2 wherein said at least one product is selected from a group consisting of a system chipset, a PCI/ISA card, a ROM, a CMOS, a CPU, a computer peripheral device, and the combination thereof.

4. A method according to claim 3 wherein said system chipset is selected from a group consisting of a clock generator, a South Bridge chipset, a North Bridge chipset, a Communication chipset, a Super I/O chipset, a Video Graphics Array chipset, a small computer system interface chipset, a Local

Area network chipset, a sensor chipset, a health chipset, a PCI/PCI Bridge chipset, an IDE ATA Controller chipset, a PCI/ISA Bridge chipset, a 1394 chipset, and the combination thereof.

5. A method according to claim 3 wherein said PCI/ISA card is selected from a group consisting of a sound card, a TV card, a VGA card, a SCSI card, a LAN card, an IDE card, an AMR card, a CNR card, a Modem card, and the combination thereof.

6. A method according to claim 3 wherein said ROM is selected from a group consisting of an EEPROM, an EPROM, a PROM, a ROM, a Flash Memory, and the combination thereof.

7. A method according to claim 6 wherein the product characteristic value of said ROM is based on one data selected from a group consisting of a Checksum value, a Class code, a Sub-class code, a Revision ID, a Device ID, a Vendor ID, a Manufacturer ID, a Product ID, a Sub-Product ID, a Sub-Device ID, a Sub-Vendor ID, a ROM Signature, a Data Structure Length, a Data Structure Revision, an Image Length, a Revision Level of Code/Data, a code Type, a Command Code, a Control Register, a Status Register, an Expansion ROM Base Address, a Configuration type, a Serial Presence Detect Data, a Clockgen device related data, and a specific address data.

8. A method according to claim 3 wherein said CMOS is used for storing a relevant set value of said BIOS.

9. A method according to claim 3 wherein said product characteristic value is selected from a group consisting of an ID, a Patch ID, a relevant register value of said CPU, and combination thereof.

10. A method according to claim 3 wherein said computer peripheral device is selected from a group consisting of a Modem, a Printer, a Serial Port Device,

a Parallel port device, a SCSI Device, an IDE Device, a UBS Device, a midi Device, and the combination thereof.

11. A method according to claim 10 wherein said SCSI Device, said IDE Device, and said USB Device are provided by a group consisting one of a diskette, a hard disk, a compact disc, a ZIP disk, a LS-120 disk, a type, and the combination thereof.

12. A method according to claim 11 wherein said product characteristic value is one selected from a group consisting of a register value, an I/O port value and the combination thereof in said at least one product.

13. A method according to claim 1 wherein said algorithm is a secret code algorithm.

14. A method according to claim 13 wherein said secret code algorithm is one of a summing algorithm and an operating function algorithm.

15. A method according to claim 1 wherein said protecting action is to skip said specific one of said program area and said data area.

16. A method according to claim 1 wherein said protecting action is to shutdown the operating system.

17. A method according to claim 1 wherein said protecting action is to halt the operating system.

18. A method according to claim 1 wherein said protecting action is to produce a flag signal to be stored in a storage device for protecting said specific one of said specific program area and data area.

19. A method according to claim 1 wherein said program area and said data area are stored in a storage module.

20. A method according to claim 1 wherein said operation value is one of a specific value and a supplemental value.

21. A method for protecting a specific one of a program area and a dada area having specific usage standards to be applied to a basic input/output system (BIOS), wherein said basic input/output system defines a mapping table therein, said method comprising steps of:

providing at least one product and reading a product characteristic value of said at least one product;

comparing said product characteristic value with said mapping table to decide whether said at least one product has said characteristic value conforming to usage standards of said specific one of said program area and said data area; and

executing a protection action for said specific one of said program area and said data area when said at least one product does not have said characteristic value conforming to said usage standards of said specific one of said program area and said data area, thereby preventing said specific one of said program area and said data area from being misappropriated illegally.